White paper

Remote access in industrial control systems

Best practice recommendations

Learn more about

- Remote access overview
- Common security pitfalls
- Practical challenges
- Best practice recommendations
- Key benefits
- Remote access und cybersecurity solutions

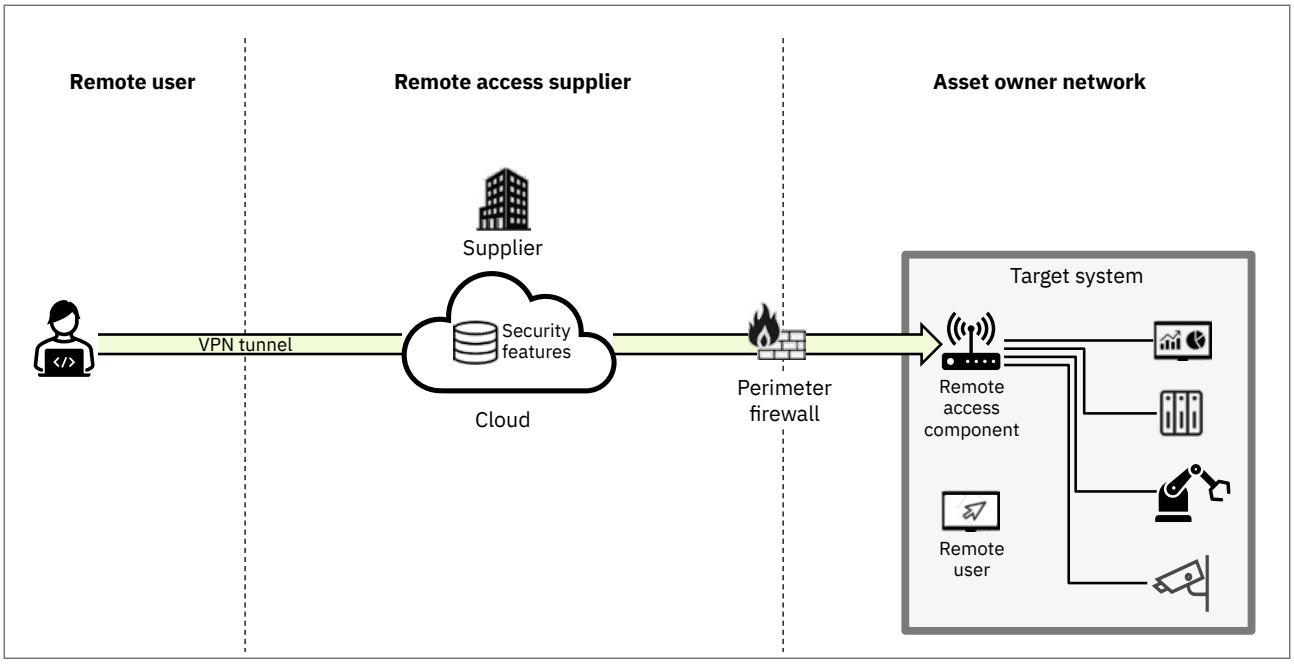
Introduction

Remote access is an integral part of Industrial Control Systems (ICS), enabling operators, engineers, and technicians to monitor, troubleshoot, and manage systems from a distance. While remote access offers convenience and has been widely adopted by asset owners, machine builders, and service providers, it must be properly integrated and secured to prevent unauthorized access and cyber threats. This white paper highlights common security pitfalls and practical challenges, and provides best practice recommendations to enhance the **security**, **flexibility**, **consistency**, and **availability** of remote access in ICS environments.

Remote access overview

Remote access typically uses VPN technology (or similar methods) to create a secure tunnel between a remote user and a target system, enabling communication as if both were on the same network. The connection is set up through a remote access component, which may be a hardware device such as an IoT gateway or firewall, or a software module installed on a controller, edge computer, workstation, or HMI panel. A common approach is remote desktop, allowing remote users to interact with the system as if they were sitting in front of it.

Remote access tunnels can be set up with or without a supplier-managed cloud. Cloud-based solutions have become mainstream as they simplify complex IT configurations and offer added security features. However, cloud reliance introduces specific security considerations that must be addressed.



Common security pitfalls

1. **Lack of segmentation**
   A common mistake is connecting remote access components directly to the ICS without proper isolation. These components communicate with external suppliers or the internet in the background, which increases vulnerability to cyber threats if not properly segmented.

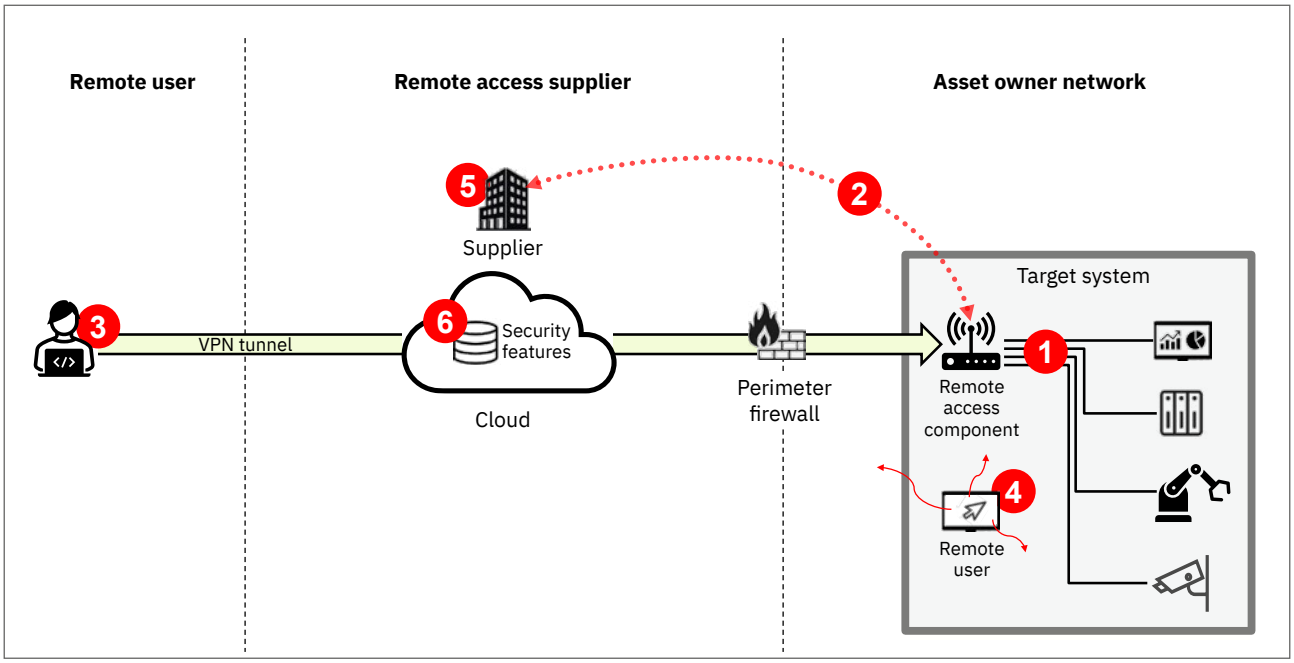
2. **Unsecured backdoors**
   Remote access devices with direct internet connectivity, especially those using cellular networks, can bypass perimeter firewalls and create hidden entry points. Multiple backdoors might exist in a facility when machine builders add their own remote access solutions.

3. **Trust-by-default**
   When remote access tunnels are established, a remote user and the target system are connected into the same network and inherently trust each other. The system often grants the remote users broad, unrestricted access and allows them to navigate the system with few or no restrictions.

4. **Excessive access**
   In the absence of granular access control, remote users often receive more privileges than necessary. Especially, a remote desktop session may inadvertently allow access to broader parts of the owner's network or even the internet.

5. **Over-reliance on cloud-based security**
   Although cloud-based remote access solutions offer built-in security features, relying on these features places security control in the hands of the supplier. This exposes the system to cloud-specific threats and supply chain attacks.

6. **Generic, not tailored security**
   Another drawback of cloud-based security is not easy to adapt to different systems with varied configurations and requirements. Often the security rules configured in the cloud are generic, not tailored to the target system.



Practical challenges

ICS environments are characterized by long lifecycles and multiple stakeholders, such as asset owners, machine builders, service providers, and others. Besides technical considerations, real-life challenges include:

Diversity
An asset owner may have multiple plants, each with diverse machinery from various suppliers. Similarly, machine builders produce a range of machine types with different configurations. Managing security across such diversity is complex.

Flexibility
Remote access is an integral part of ICS and is subject to change. For example, machine builders may favor one platform, while asset owners demand another. Other scenarios that cause change include technology shifts, budget constraints, or supplier considerations. However, users are often tied to their supplier cloud platforms, making transitions between platforms difficult.

Consistency
Keeping security rules and policies consistent while meeting diversity and flexibility is challenging. For instance, how can machine builders keep the same access control policies, user account management, and permission enforcement regardless of which remote access solution the asset owners demand for?

Availability
ICS systems are expected to run over extended periods. Remote access cloud service outages, cyberattacks, or supplier discontinuation cause downtime and pose significant impact on business. Ensuring system resilience is both a technical and operational imperative.

Best practice recommendations

1. **Segment your system into zones**
   Follow the Purdue model and the IEC 62443 standard, segment your system into zones and conduits. This approach restricts data flow, prevents lateral movement, and forms the foundation for secure remote access.

2. **Separate remote access from your system**
   Remote access components transfer user data and background traffic to the supplier and internet as well. It is crucial to treat them as untrusted and separate them from the core system. Isolation reduces the system's exposure to external threats.

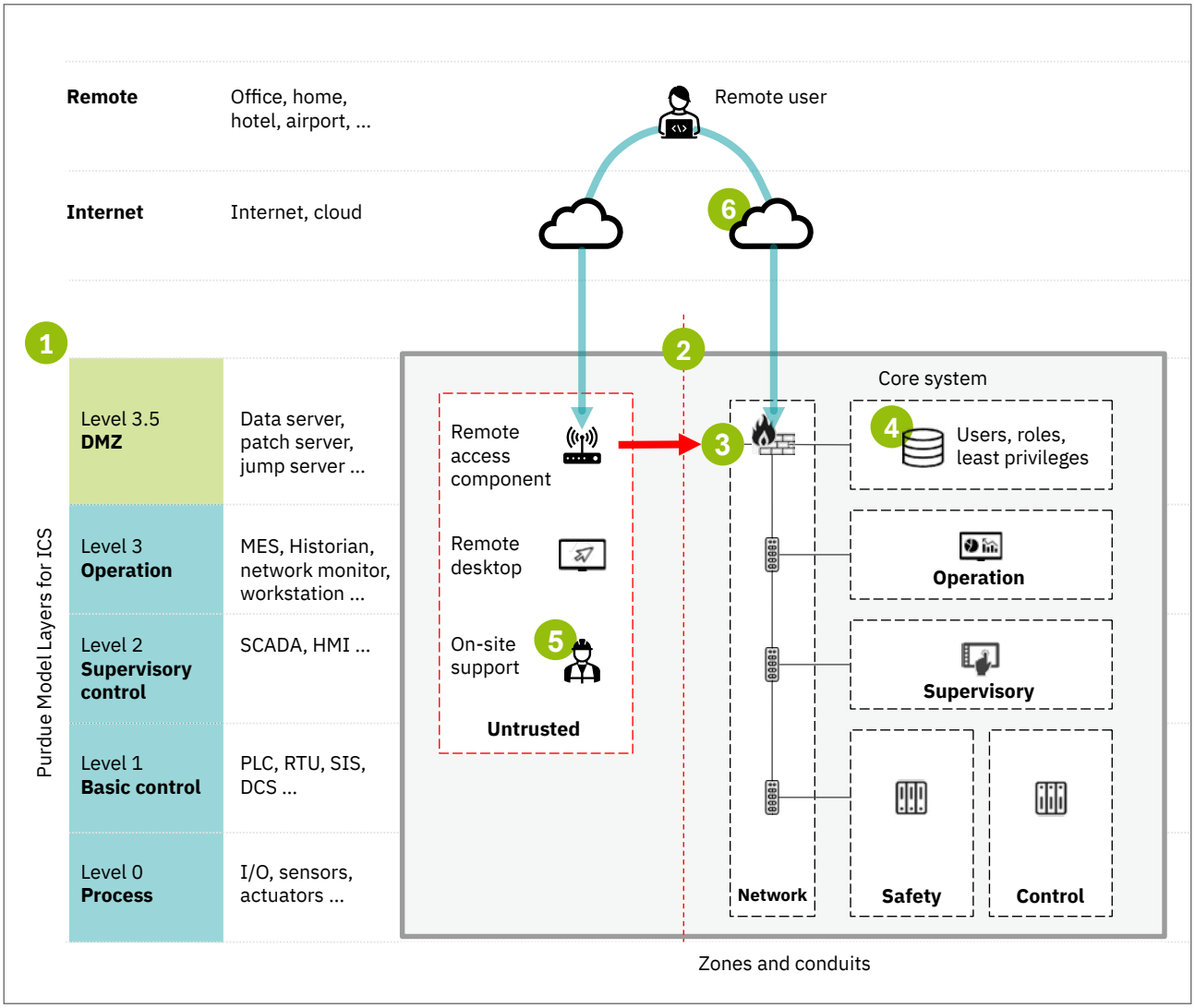
3. **Minimize the surface to remote access**
   Apply the principle of minimizing the attack surface. Limit the surface of remote access. Ideally, remote access should be funnelled through a single, designated port. This simplifies security access control, reduces complexity, and enhances threat mitigation.

4. **Implement system-based security**
   Rather than over-reliance on cloud-based security, build access control mechanisms into the system itself at the designated port. This ensures consistent security across diverse deployments regardless of the remote access

platform. Implement principles like “deny-by-default, allow-by-exception,” “role-based access control,” and “least privilege.” A connected remote user should remain blocked unless authenticated and authorized according to system-specific rules (not the generic rules in the cloud).

5. **Unify remote and on-site access surface**
   Remote and on-site users often perform similar functions, such as monitoring and maintenance. Standardize the access surface and security rules for both, thereby reducing complexity and internal threat vectors.

6. **Integrate redundancy with a second source**
   Integrate a secondary remote access solution from an alternative supplier to maintain availability in case of service disruption. Use the same security rules for both primary and secondary paths to prevent duplication of effort or inconsistent configuration.



Key benefits

Security
- Aligns with Purdue model and IEC 62443 design principles
- Creates secure zones and conduits to prevent lateral movement
- Separates untrusted remote access from core systems
- Minimizes the remote access attack surface
- Enables system-based security, rather than cloud-based security
- Enables tailored security to the system, not generic security in the cloud
- Enforces zero-trust concept, deny-by-default, allows by exception
- Builds in role-based access control and least privilege principles

Flexibility
- Avoids vendor lock-in, not bundled to any specific remote access supplier
- Adapts to any remote access platform
- Simplifies transition between platforms and suppliers

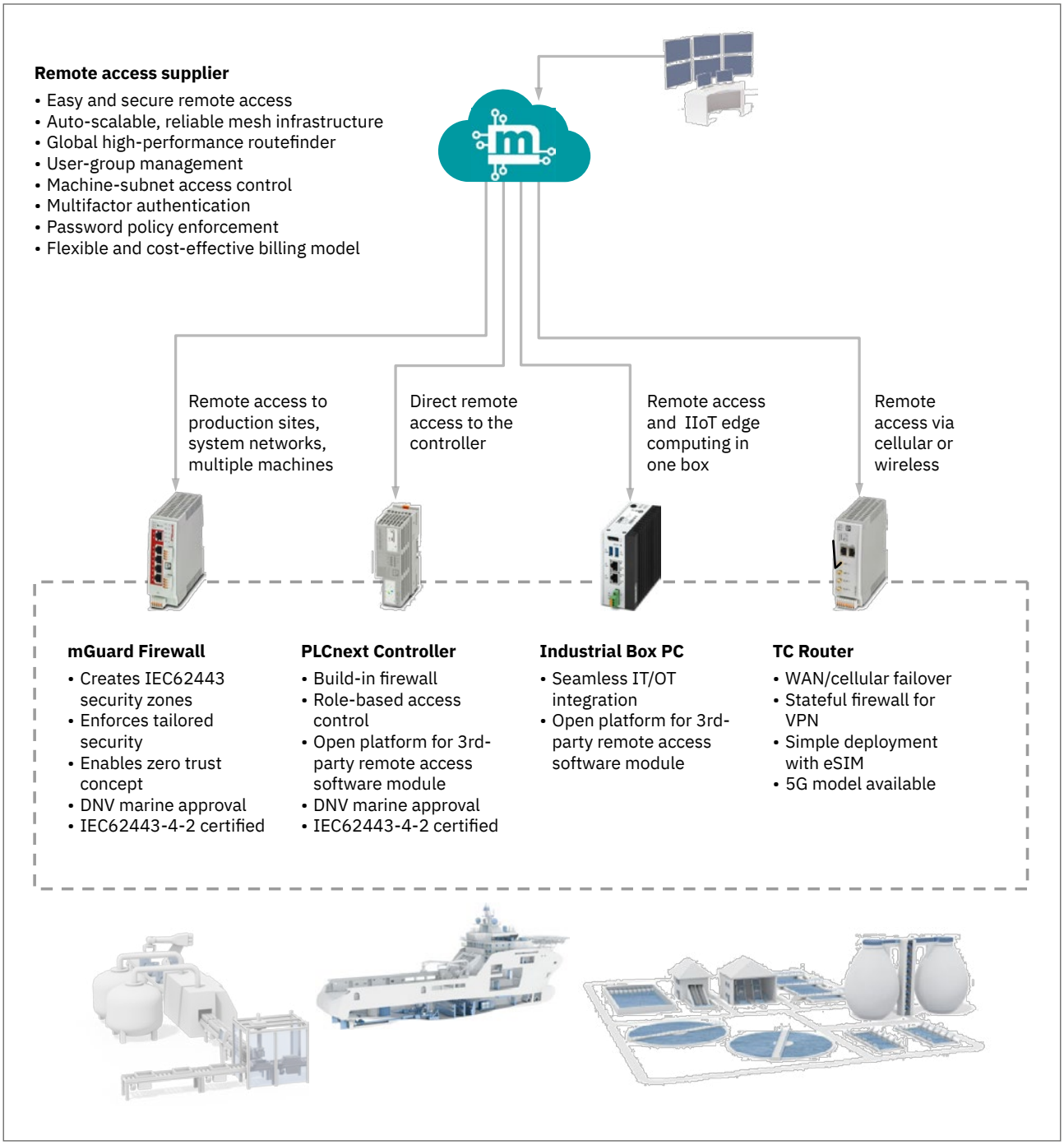
Consistency
- Ensures consistent security rules regardless which remote access platform is used
- Standardizes security rules for remote and on-site users
- Unified access rules for primary and redundant remote access paths

Availability
- Enhances system resilience with a redundant remote access
- Mitigates risks from cloud outages and supplier discontinuities

Phoenix Contact remote access and cybersecurity solutions

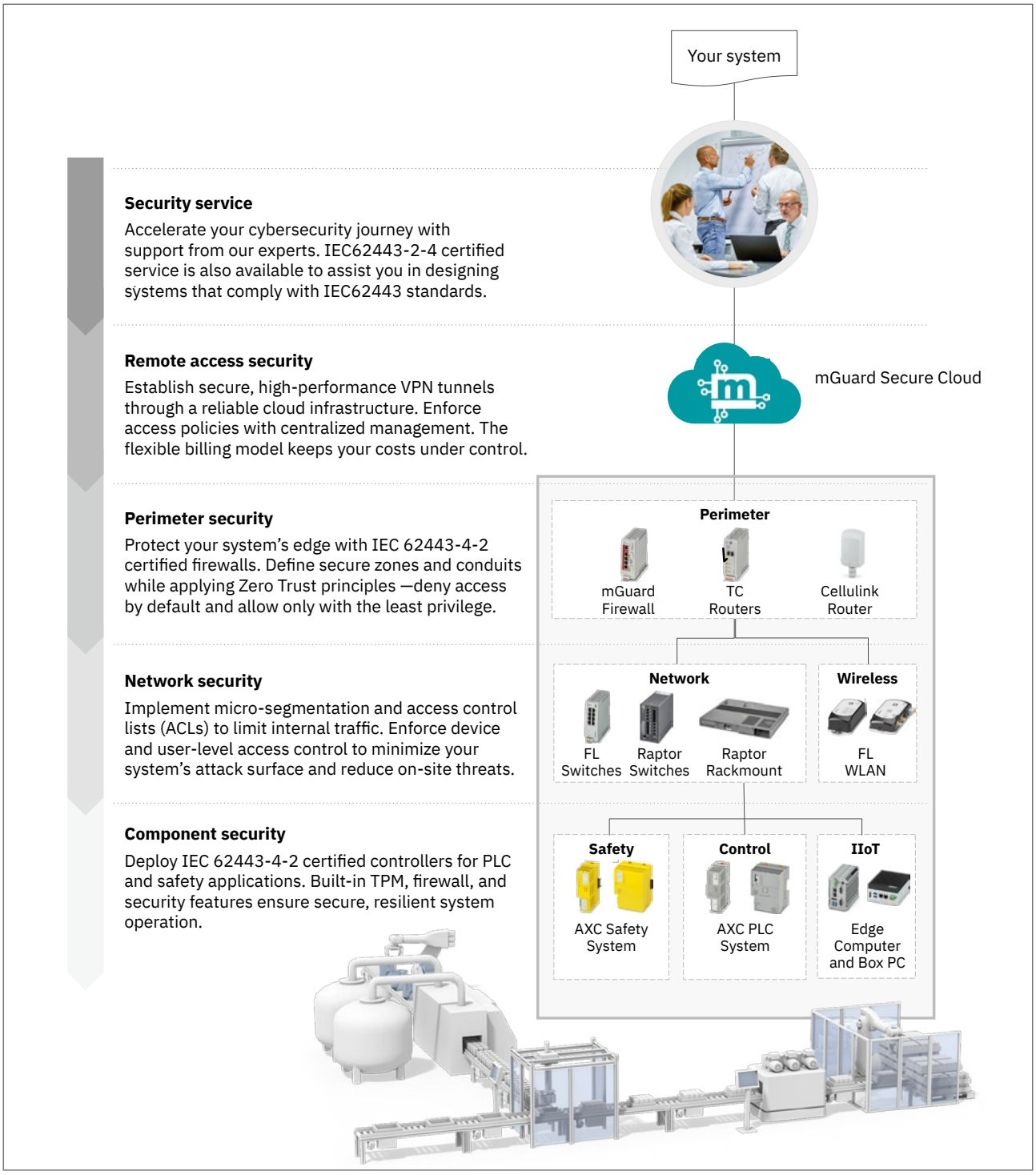
mGuard Secure Cloud

Phoenix Contact's cloud service enables simple and secure remote access that fits all your needs, from a simple VPN client to extensive system networks.



Defense-in-depth for your remote-access-enabled system

Phoenix Contact has been implementing IEC 62443 standards since 2017, delivering cybersecurity services, solutions, and products to help you design and implement defense-in-depth – from remote access and perimeter protection to network and component security to ensure the secure and robust operation of your industrial control system.



Contact

We recommend starting with our Cybersecurity Assessment and Advisory Service. Work with our Network & Cybersecurity Specialists to evaluate your system's risk profile and receive expert guidance on IEC62443, network segmentation, modular architectures, and multi-layered defence, as well as secure remote access.

For more information, please contact us.

JJ Sun
Network & Cybersecurity Specialist
TÜV Rheinland Cyber Security training program certified specialist with 20 years of experience in industrial networking
jsun@phoenixcontact.com

Why Phoenix Contact
Cybersecurity is a journey and Phoenix Contact is your trustworthy supplier with a leading pace towards NIS2, CRA, IEC 62443. We develop technologies and manufacture security products and use them to secure our worldwide production sites – as well as yours.

Your benefits
Cybersecurity requires a holistic approach. Our 360° security, from product, solution to service, is a fast track for securing your system with Network, Safety, Automation, and IIoT – all from one place.

phoenixcontact.com

2025-08-15/00
3012721056